REMARKS

This amendment is in response to the Official Action dated June 19, 2007. Claims 9, 12, and 17 have been amended, claims 5-8, 10, and 13 have been canceled, and claims 18-24 have been added; as such claims 1-4, 9, 11-24 are now pending in this application. Claims 1-4, 9, 14, 18, 20, and 22 are independent claims. Reconsideration and allowance is requested in view of the claim amendments and the following remarks.

No new matter has been added by this Amendment. Support for the new claims can be found in Fig. 1 and the corresponding portion of the specification as filed.

Applicant thanks the Examiner for the acknowledgement of priority under 35 USC § 119.

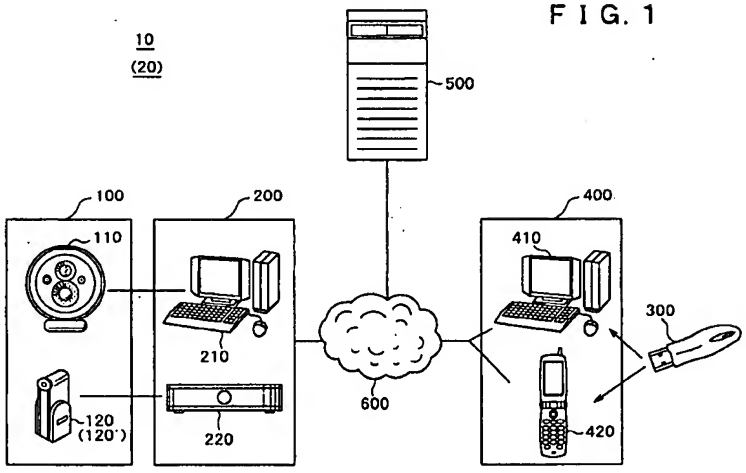
Applicant acknowledges and thanks the Examiner for the consideration of all of the references listed in the Information Disclosure Statement filed April 23, 2007.

An Example Embodiment

Fig. 1 illustrates an example embodiment of the present invention, including an image pickup device 100, a key generator device 200, an authentication server 500, a viewer device 400, and a memory card 300. The image pickup device may include a USB camera 110 or an IP camera 120. The key generator includes a computer 210 and a router 220. Initially, key generator 200 produces a pair of complementary encryption and decryption keys. The encryption key is stored to an image pickup device and the decryption key is stored on the memory card, which at the time is connected to the key generator. Thereafter, the key generator 200 registers a number identifying the image pickup apparatus with authentication server 500. To view images from image pickup apparatus 100 on the viewer apparatus 400, the user first is authenticated by the authentication server 500 in response to an authentication request from the viewer device 400. Thereafter, if the unique identifying number in the memory card 300 corresponds to the desired image pickup device, the viewer connects to the pickup image device 100. The image pickup device 100 then transfers

encrypted images to the viewer device 400. The viewer 400 uses the decryption key in the memory card 300 to decrypt the images from the pickup image device.

FIG. 1



Rejections under 35 U.S.C. § 101

Claim 17 has been rejected under 35 U.S.C. § 101. Applicant submits that claim 17 has been amended to overcome the rejection.

Rejections under 35 U.S.C. 102(b)

Claims 5-7 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Publication No. 2002/0060736 to Wakao et al ("Wakao").

Applicant submits this rejection is moot as claims 5-7 have been cancelled.

Rejections under 35 U.S.C. 103(a)

Claims 1-4 and 9-12 have been rejected under 35 USC § 103(a) as being unpatentable over Wakao in view of U.S. Patent No. 7,136,487 Schon et al. ("Schon")

Wakao discloses an image data verification system that determines whether images generated by an image device, e.g., a digital camera, have been altered or not without significantly impacting the performance of the image generation device. Fig. 4 illustrates the components of the image verification device including an image generation device 10, a verification data converting device 20, and an image verification device 30. Wakao discloses that the program memory 17 stores common information for generating primary verification data, i.e., an encryption key (Wakao at paragraph 43). However, Wakao does not indicate where the encryption key comes from nor does Wakao disclose the creation of a decryption key at the same time. Furthermore, Wakao does not disclose a viewer connected to the camera via a network or an authentication server accessible by a viewer.

Schon discloses a method of protecting private video content using embedded cryptography security. Fig. 4 illustrates a digital camera having removable memory 51 and video casset 50. Removable memory 50 includes an encryption program 53 and encryption key 54. During operation, digital video camera 41 uses the encryption program 53 to encrypt the digital content stored on videocassette 50 (Schon at column 7, lines 8-18). Figure 5 illustrates a digital video player 61, video cassette 69 and removable memory 70. Removable memory 70 includes a decryption program 72 and decryption key 73. Videocassette 69 has encrypted digital video content. To play the contents of videocassette 69, the digital video player 61 uses program 72 and decryption key 73 to decrypt the digital video content in videocassette 69. However, like Wakao, Schon fails to disclose either a key generator in communication with a camera, a viewer connected to the camera via a network, or an authentication server accessible by a viewer.

Claim 1 recites: *[a]n image transmission system for transmitting an image via a network, said image transmission system comprising:*

one or a plurality of image pickup apparatus each having a unique identifying number and having an encrypting function for encrypting a picked-up image for transmission to said network;

a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for encrypting said image and a decryption key for decrypting said encrypted image;

a removable recording medium for recording said decryption key and the identifying number of said image pickup apparatus in association with each other;

a viewing apparatus connected with said removable recording medium and having a decrypting function for decrypting said encrypted image using said decryption key, for viewing the image transmitted via said network by said image pickup apparatus; and

an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.

"a viewing apparatus... for viewing the image transmitted via said network by said image pickup apparatus"

Neither Wakao nor Schon teach or suggest "*a viewing apparatus ... having a decrypting function for decrypting said encrypted image... for viewing the image transmitted via said network by said image pickup apparatus*" In claim 1, the viewing apparatus is viewing images transmitted over the disclosed network from the image pickup apparatus.

Page 6 of the outstanding office action asserts that paragraph 45 of Wakao discloses "an apparatus (20) connected with said recording medium and having a decrypting function for decrypting said encrypted image using said decryption key." With respect to cryptography, paragraph 45 recites that table T1 is stored on program memory 26, and includes specific IDs of a plurality of image generation devices, a plurality of pieces of common information Kc corresponding to the respective specific IDs, each of which is equivalent to the decode key of the

common key cryptography, and a plurality of pieces of secret information Ks corresponding to the respective IDs, each of which is equivalent to the secret key of a public key cryptography." Nowhere is it recited that apparatus 20, which is connected to the image device, decrypts the image. On the contrary, apparatus 20 is one of the components involved in converting the image from the image device by adding the second layer of verification data.

Furthermore, the output unit 22 in paragraph 45 of Wakao "outputs a message showing whether or not the image file with secondary verification data is altered." There is no suggestion that the output unit provides a decrypted view of the image.

Accordingly, Wakao does not provide an image viewer. At best, Wakao only discloses an output display for showing a status indicator for the verification process.

Furthermore, Schon also does not disclose a viewer "*for viewing the image transmitted via said network by said image pickup apparatus*" because the Digital Video Player 61 disclosed in Schon only plays back data from the disclosed digital videocassette 69. Schon does not disclose receiving data from the imaging device at the Video Player 61 via a network.

Accordingly, neither Wakao nor Schon teach or suggest "*a viewing apparatus connected with said removable recording medium and having a decrypting function for decrypting said encrypted image using said decryption key, for viewing the image transmitted via said network by said image pickup apparatus,*" Even assuming, arguendo, that Pierrat and Shioiri were combinable, none of the cited references, either alone or in any proper combination, cure the deficiencies of Pierrat with respect to at least the previously identified features of independent claims 1, 6, and 11 because there is no suggestion of this missing feature.

"an authenticating server..."

Neither Wakao nor Schon teach or suggest *"an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus."* That is, neither Wakao nor Schon disclose an authentication server accessible from the viewing apparatus.

Page 6 asserts that the image verification device 30 disclosed in Wakao is equivalent to the authentication server of claim 1, and that the image verification device is accessible by apparatus 20. However, as set forth above, apparatus 20 fails to meet the requirements of the disclosed apparatus.

Furthermore, even if apparatus 20 of Wakao was comparable to the viewing apparatus of claim 1, Wakao would still fail to meet the requirements of the authentication server. In particular, the image verification device 30 serves to verify an image based on encryption data. The image verification device 30 does not serve to authenticate an image pickup apparatus. The verification device in Wakao provides further layers of verification on the image from the imaging device 10, it does not authenticate the imaging device itself.

Schon also does not disclose an authentication server, in particular, because the digital video player uses program 72 in removable memory to decrypt video digital cassette images without reference to the imaging device. That is, the player in Schon will play the digital content on video cassette 69 so long as the removable memory contains the proper decryption key for the video content.

Accordingly, neither Wakao nor Schon teach or suggest "*an authenticating server for authenticating said image pickup apparatus accessible from said viewing apparatus.*" Even assuming, arguendo, that Pierrat and Shioiri were combinable, none of the cited references either alone or in any proper combination, cure the deficiencies of Pierrat with respect to at least the previously identified features of independent claims 1, 6, and 11 because there is no suggestion of this missing feature.

"a key generating apparatus..."

Neither Wakao nor Schon teach or suggest "*a key generating apparatus for generating, for each said image pickup apparatus, an encryption key for encrypting said image and a decryption key for decrypting said encrypted image.*" In claim 1, the key generating apparatus that generates an encryption key and decryption key for each of the image pickup apparatuses.

Page 5 of the office action alleges that Wakao discloses a key generating apparatus as disclosed in claim 1. However, even the disclosed office action fails to cite to a reference numeral or page showing a key generating device or apparatus. Instead, the office action only states that "an encryption key is generated for each image pickup apparatus." However, the Office Action does not disclose, nor does Wakao contain a key generating apparatus.

Schon fails to disclose a key generating apparatus. While Schon discloses the use of memory cards containing encryption/decryption keys, Schon does not disclose the source of the encryption/decryption keys.

Accordingly, neither Wakao nor Schon discloses a key generating apparatus. Therefore, even assuming, arguendo, that Pierrat and Shioiri were combinable, none of the cited references either alone or in any proper combination, cure the deficiencies of Pierrat with respect to at least the previously identified features of independent claims 1, 6, and 11 because there is no suggestion of this missing feature.

Since even a combination of the relied upon references would still fail to yield the claimed invention, Applicant submits that a prima facie case of obviousness for claims 1, 6, and 11 has not been presented. Therefore, withdrawal of the rejection of these claims and any claims dependent thereon is respectfully requested.

CONCLUSION

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-2960 from which the undersigned is authorized to draw.

Dated: September 27, 2007

Respectfully submitted,

By_____
Ronald P. Kananen
Registration No.: 24,104
Christopher M. Tobin
Registration No.: 40,290
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 23353
Attorneys for Applicant